# Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks

**Shafiullah Khan, Kok-Keong Loo**

**School of Engineering and Design, Brunel University, UK**
**Kohat University of Science and Technology (Kust), Pakistan**

**IEEE 802.11 WMN is an emerging next generation low-cost multi-hop wireless broadband provisioning technology. It has the capability of integrating wired and wireless networks such as LANs, IEEE 802.11 WLANs, IEEE 802.16 WMANs, and sensor networks. This kind of integration: large-scale coverage, decentralised and multi-hop architecture, multi-radios, multi-channel assignments, ad hoc connectivity support the maximum freedom of users to join or leave the network from anywhere and at anytime has made the situation far more complex. As a result broadband resources are exposed to various kinds of security attacks, particularly DoS attacks.**

## 1. Introduction

The main objective of DoS attacks is either to completely tie up certain resources or to bring down an entire network so that the legitimate users are not able to access service(s). Flooding, one of the most sophisticated types of DoS attack, is spreading faster and causing more damage. Flooding exploits the huge resource asymmetry between the internet and the victim.

Detection and prevention of such attacks and misuses is of prime importance and it is a complex task because these attacks can be conducted anywhere and at anytime with varying intensity, particularly in the wireless mesh network (WMN) environment. Intrusion detection systems can be used to detect such flooding attacks; however, they may have a high incidence of false alarms. Current rules-based and anomaly-based intrusion detection systems detect intrusions either by matching patterns of network and users activities with pre-defined rules or they define the normal profile of system usages and then look for deviation.[1] These approaches have their consequences and drawbacks. The former is well suited for known intrusions but it cannot detect new intrusions. The latter relies on deviation from normal usage and sometimes fails to detect well known intrusions.

In recent years, some well known websites, for example ebay.com and yahoo.com, were down for some time following successful distributed flooding attacks. The ultimate objective of such attacks is to make services unavailable to legitimate users.

The research community has proposed some important security mechanisms to detect flooding attacks at the TCP/IP layer, as wire-line networks (such as local LANs) are only vulnerable to network and transport layer flooding attacks such as UDP flood, ICMP flood, and IGMP flood. However, an adversary can launch not only TCP/IP layer flooding attacks but also MAC layer flooding attacks, such as probe-request flood and de-authentication flood against IEEE 802.11 WMN. Multi-layer flooding attacks can be detected using a cross-layer approach.

This paper introduces a real-time cross-layer flood detection and attack trace-back mechanism, RCFDAT, for WMN, which is based on a feature set formed from selected cross-layer parameters of different layers. RCFDAT analyses the parametric values and, once it detects the ongoing flooding attack, checks the severity and intensity of that attack by observing resources utilisation. The calculated statistics show that RCFDAT has a remarkable detection rate with low false alarms.

The remaining part of this paper is organised as follows: Section 2 describes related work in detecting flooding and associated attacks. Section 3 gives overview of different flooding attacks and possible techniques in WMN. Section 4 explains the working mechanism of RCFDAT. Section 5 shows simulations and results. Section 6 concludes the paper.

## 2. Related work

Most hosts are prone to flooding attacks over the internet, and prevention mechanisms have been proposed to reduce the damages.[3,4] Firewalls are one solution and ingress/ egress traffic filtering mechanisms fall under this category.[5,6,7] Another is

an on-off feedback control strategy that defends against distributed denial of service attacks – based on backward propagation.[8] The impact of DoS attacks on multicast protocols has been analysed and the weaknesses of traditional gossip-based multicast protocols have been evaluated.[9]

Most research has focused on analysing the network traffic pattern of flooding attacks.[10,11,12] A flood prevention mechanism has been proposed using route-based filtering which requires routing and topological information to mark the packet valid with respect to source and destination addresses.[13] Some research has been carried out to trace back the flooding attack path. This research has generally been based on IP trace back mechanisms, which are not efficient enough to detect spoofed flooding attacks.[14,15,16,17] Wavelet methods have been proposed, which capture high bandwidth flows to check the wavelet variance resulting from attack traffic.[2, 18]

Another proposed flood detection method observes TCP control and data packets.[19] The method is based on the assumption that during a SYN flooding attack, the number of SYN packets greatly increases compared to FIN packets. However, this mechanism is able to detect only SYN flooding. An improved version extends the capability to detect other forms of flooding attacks by considering TCP flag rates and protocol rates.[20] This mechanism is based on the philosophy that the number of TCP packets with specific flags drastically changes or the number of IP packets sharply increases when flooding attacks occur. However, these mechanisms are unable to detect low-rate TCP targeted DoS attacks, in which TCP/IP traffic does not sharply increase because attackers keep the intensity low.[21] Furthermore they cannot classify the flooding attacks as low-intensity flooding or severe flooding.

A more appropriate approach to detecting low-rate flooding attacks is to take into consideration the resource utilisation of the system of incoming traffic. However, rapid increase in resource utilisation may not be necessarily be due to flooding attacks. Sometimes software bugs, worms, and viruses like MS-Blast can also be the reason for a rapid increase in resource use.[22]

Most current approaches deal with flooding attacks against the TCP/IP of wired or wireless networks, such as UDP flood, SYN flood, IGMP flood, and ICMP flood. However, IEEE 802.11 WMNs and IEEE 802.11 WLANs are vulnerable to MAC layer flooding attacks such as de-authentication and probe request flood.[23,26] Cross-layer flood detection mechanism is necessary to detect the great variety of flooding attacks against the broadband services of IEEE 802.11 WMNs, and to defend against multi-layer flooding with great accuracy. Our mechanism takes parameters from the MAC layer and TCP/IP to detect the flooding attacks. Once the flooding attack is detected, then RCFDAT classifies its severity as well as traces back the attack source(s).

RCFDAT has many advantages with respect to the existing methods:

- It is capable of detecting multi-layer flooding attacks.
- It offers reduced complexity and computation.
- It classifies flooding attacks on the basis of severity such as medium, high or severe.
- It detects high flooding attacks that have a sharp increase in flows by monitoring traffic flows, while it detects low-rate flooding attacks by constantly watching resources utilisation.
- It traces back the attacking source(s).

# 3. Flooding attacks

In a single node flooding attack, a single host is used, while in distributed flooding, multiple infected systems are used to carry out flooding to heavily congest the network. The attacker prevents the access of legitimate users to broadband services. In such attacks, the attackers are well protected, and they use a public network for flooding to bring about these disasters. IEEE 802.11 is more vulnerable to such flooding attacks due to the large-scale community-based coverage – decentralised architecture in which the attacker can launch such attacks from anywhere anytime. Furthermore end users are connected with the Mesh Gateway (MG) through the multi-hop backbone of Access Points (APs) or Wireless Mesh Routers (WMRs). This kind of multi-hop decentralised architecture makes it easier for attackers to launch three types of network layer flooding attacks.

## Single node flooding against AP or WMR

In this type of attack, a single node starts flooding against the AP or WMR. The purpose of such an attack is to exhaust the computation as well as bandwidth resources. However, this type of attack is not so severe.

## Distributed flooding against AP or WMR

Normally, an AP is capable of serving approximately 30 nodes. When many nodes that are in the direct communication range of an AP start flooding, this may seriously degrade the normal operations of AP in terms of bandwidth, CPU, memory, and other resources. This kind of attack is also capable of bringing down the target AP by denying broadband services to legitimate users.

## Distributed flooding against MG

This is the most severe flooding attack against IEEE 802.11 WMN, in which multiple attack sources scattered around start flooding against the MG through the multi-hop backbone of APs. Such an attack may heavily congest the whole network. Furthermore, if this kind of attack is more severe it may result in the crash of the MG. If this occurs the whole network will be down for all legitimate users.

Distributed flooding attacks can be launched by a highly skilled programmer and there is need for a high degree of interaction and collaboration amongst infected systems which are termed 'zombies' and the attacker. Intermediate nodes are used for such collaboration as shown in figure 1. The attacker establishes a connection with the intermediate node and instructs to launch a distributed flooding attack. The intermediate node, after receiving the launching com-

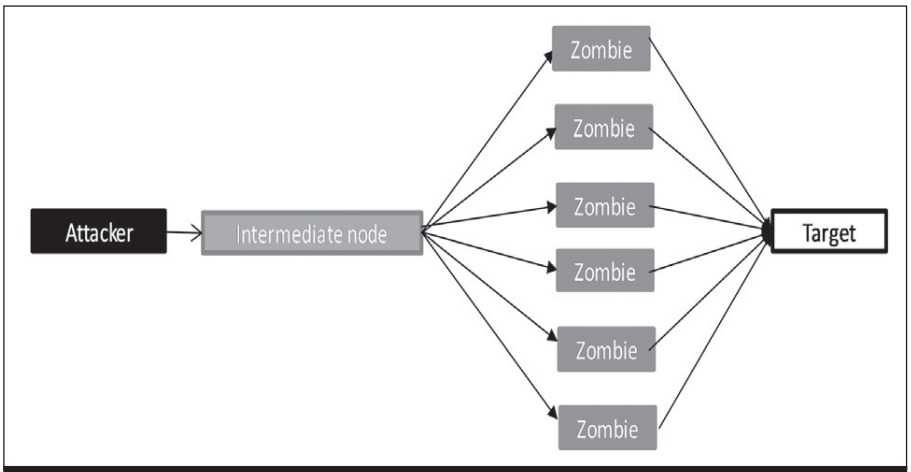


Figure 1: Distributed flooding attack mechanism.

mand, sends a query to all zombies to check their status. Each zombie sends an acknowledgement to the intermediate node that it is ready for the attack. Once the intermediate node receives such an acknowledgement it instructs the zombies to start flooding toward the target.[24]

The objectives of such attacks may be to overflow the bandwidth, memory, computational, or connection buffer and may result in zero-service for all legitimate users. Zero-service is a situation in which legitimate users are unable to access the network or network resources after a severe attack. The distributed flooding can be further classified on the basis of protocol used.

### UDP Flood

In a UDP flooding attack, the attacker mostly uses techniques like TRINOO and Shaft.[25] The communication between attacker and intermediate node is usually done by TCP, while UDP is used for communication between the intermediate node and the zombies. The zombies start flooding UDP packets towards the target once they receive the attack command from the intermediate node.

### SYN Flood

In a SYN flooding attack, the attacker exploits the three-way handshake of the TCP mechanism. The attacker never completes the three-way handshake mechanism but requests the connection again and again using a spoofed IP and heavily overloads the target. The attacker mostly uses techniques like Tribe Flood Network (TFN) and TFN2K. The communication between the attacker and intermediate node is usually done by either command line interface or encrypted communication using a key-based CAST-256 algorithm, while ICMP echo or UDP is used for communication between the intermediate node and the zombies.[25] The zombies start flooding towards the target, and heavily overload its memory, computation, and bandwidth resources. The attacker can also use TFN and TFN2K to launch UDP and ICMP flooding attacks.

### ICMP Flood

ICMP flood, also known as Ping flood or Smurf attack, is a type of DoS attack that sends large amounts of oversized ICMP packets with the aim of crashing the TCP/IP stack on the machine and causing it to stop responding to TCP/IP requests. The commonly used techniques to carry out this kind of flooding attack are TFN and stacheldraht. In stacheldraht, an encrypted TCP connection is used for communication between the attacker and intermediate nodes. ICMP echo is usually used by the intermediate node to instruct the zombies to launch the flooding attack.

### Probe Request Flood

Probe request frames are used by client nodes to discover a wireless network in IEEE 802.11 WMN and WLAN. If a wireless network exists then the AP responds with a probe response frame. The attacker can send a flood of probe request frames using MAC spoofing to represent a large number of nodes scanning for the wireless network, which heavily overloads and consumes the computation power and memory resources of the AP.

### De-authentication Flood

Another flooding attack that may result in service unavailability to legitimate users is the de-authentication attack. The IEEE 802.11 client first authenticates with the AP before the start of communication. After that, the client needs to send a de-authentication message to the AP to terminate the communication. This de-authentication message is itself not authenticated. The attacker may spoof a flood of such messages and the AP would then stop its communication with a large number of legitimate nodes until the authentication is re-established. The AP cannot refuse the de-authentication as it is a notification by the client to an AP to stop the communication.

## 4. Real-time cross-layer flood detection and attack trace-back mechanism (RCFDAT)

The motivation for the proposed mechanism is based on the following facts:

- Due to inherent vulnerable characteristics, IEEE 802.11 WMN is more vulnerable to flooding-type attacks as compared to wired or single-hop wireless networks.
- The unique type of MAC layer flooding such as probe-request flooding and de-authentication flooding may result in denial of service(s).
- The attacker has the flexibility to use static as well as mobile zombies.
- In case of distributed flooding, if the attack intensity is greater than the total resources of MG, this may result in a complete collapse of broadband services.
- If a flooding attack does not completely collapse the MG, however, the multi-hop backbone may still face serious congestion.

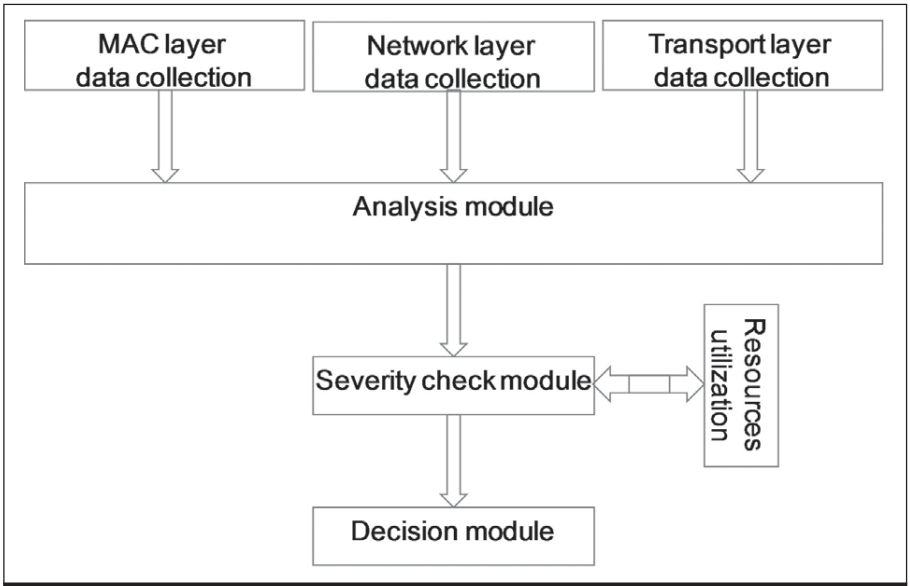


Figure 2: Block diagram of RCFDAT.

- To avoid large scale exploitation at the MG, it is necessary to have a flood detection and alarm mechanism in APs or WMR in order to detect such attacks near the source(s). Such implementation not only protects the MG but also avoids congestion at the multi-hop backbone.
- A cross-layer flood detection mechanism would be a contender for detecting both network and MAC layer flooding attacks.

We aim to construct a large-scale multi-layer flood detection approach with low computational complexity, high accuracy, and low false-alarm rate – we propose the RCFDAT.

We strongly believe that a flood detection mechanism must have the following features:

- Accurate detection and minimum false alarms.
- Differentiation of flooding attacks on the basis of protocol layers.
- Classification of severity of flooding attacks such as low, medium or high intensity.
- Detection of attack sources using trace-back mechanism.

| S # | Parameters | Protocol layer |
|---|---|---|
| 1 | MAC address | Link |
| 2 | No. of probe requests and time interval between them | Link |
| 3 | No. of probe responses and time interval between them | Link |
| 4 | No. of de-authentication requests and time interval between them | Link |
| 5 | No. of de-authentication responses and time interval between them | Link |
| 6 | Sequence Control field | Link |
| 7 | TCP/IP protocol used (UDP, ICMP, IGMP) | Transport, Network |
| 8 | Packets send/received and duration | Network |
| 9 | Time To Live (TTL) | Network |
| 10 | TCP flags ratio (SYN, FIN, ACK) | Transport |
| 11 | Duration of the connection | Transport |

Table 1: Parameters.

RCFDAT uses multiple data collection and a single data analysis (MCSA) in which multiple data collection modules gather the data. The received data is analysed by a single module as shown in figure 2. This technique is computationally less expensive compared to MCMA (Multiple data Collection, Multiple Analysis).[27] Selection of parameters from different layers is a critical task in cross-layer design.

## Data collection

RCFDAT uses three separate modules for collecting data from MAC, network, and transport layers. MAC layer data is used to detect the MAC layer flooding attacks, while network as well as transport layer data is used to detect UDP, SYN, ICMP, IGMP, and other such flooding attacks. The parameters over which the RCFDAT keeps watch are given in table 1.

## Analysis module

For launching probe-request and de-authentication flooding attacks, the adversary uses the mechanism of MAC spoofing. The MAC address is an important piece of information, but unfortunately it is not encrypted which may result in management frames exploitation. For example, an adversary (A) wants to spoof the MAC address of a legitimate user (L), so that its MAC address ($M_C$(A)) matches with the legitimate user's MAC address ($M_C$(L)). By doing this, the adversary may gain full access to the network resources. The general format of MAC spoofing is shown as follows:

L∈ Legitimate user, A∈Adversary, therefore

$$M_C(L) = M_C(A) \quad (1)$$

The detection of probe-request and de-authentication flooding attacks is required to counter the MAC spoofing. The 2-byte sequence control field of management frames can greatly facilitate in this regard, in which 4-bit are used for the fragment number while 12-bit are use for the sequence number.[28] The adversary either needs to control the firmware functionality or to develop a custom firmware with

own source code to alter the value of the sequence control field in the management frames.[29] Analysing the sequence control field along with the other parameters such as the number of probe requests, probe responses, de-authentication requests, de-authentication responses, and their time intervals can identify such spoofed MAC layer flooding attacks. The constant time intervals suggest any of these flooding attacks.

Other flooding attacks such as UDP flood, SYN flood, and ICMP flood can be detected using parameters obtained from the network and transport layers. An important indication of flooding attack is a rapid increase in network traffic flow towards the target. Traffic analysis is very helpful in detecting an ongoing flooding attack or the possibility of such an attack.

The important requirement of packet analysis is to understand the underlying protocol that the packet is using. In traffic analysis the same mechanism is used as mentioned in 'Compiling network traffic into rules using soft computing methods for the detection of flooding attacks with some modifications'.[20] First the RCFDAT captures the network traffic and classifies it into TCP, UDP, ICMP, and IGMP by decoding the protocol field in its header. The numbers of packets sent/received are counted for a fixed duration. The port of the traffic is also watched in order to avoid port-level misbehaviour. In the case of the TCP, the header is checked, which contains SYN, FIN, and ACK flags. If any of the flags are turned on, the flag is counted. The source of the flooding attack can be detected using the source IP address. However, most of these attacks rely on spoofed IP addresses.

The TTL value can facilitate in detecting whether the attack is from a single source or multiple sources. In the case of a single source, the TTL value would be the same, while a variation in the TTL value would suggest that there are multiple attackers. The attack trace-back mechanism is further strengthened by using the ant system (AS) algorithm. In the AS algorithm, ants interact in a distributed manner by sharing knowledge with their neighbours. The objective of every ant is an optimal solution towards the destination. The same mechanism is used in distributed flooding attacks – all zombies have the same destination. Combining the cross-layered parametric values such as management frames, TTL, sequence number, source, and destination IP addresses with the AS algorithm can accurately detect that:

- The attack is based on single node or multi nodes.
- The distance of the attack source(s).
- The attack sources are using spoofing mechanism or not.

To indentify a flooding attack from the n parametric flows, there is a flow-table which lists such flows having rapid increase and variations.

Let $f_e$ be the set of such flows in the flow-table and Pr($\in$ i) be the probability of choosing flow i with rapid increase, and $n_i$ be the intensity of flow i.

Let $p\ (mali)$ be the probability of not choosing the innocent flow as the flooding. The node having flow under the normal threshold $\gamma$ is not stored in the flow-table. Therefore,

$$\Pr(\in i) = \text{pr}(n_i >= \gamma) = 1 - \text{pr}(n_i =< \gamma)$$
$$\Pr(n_i =< \gamma) = \text{pr}(n_i \in f_e)$$
$$\Pr(n_i \in f_e) = \text{pr}(\mu_i >= \beta)$$

Where $\mu_i$ is the flow i and $\beta$ is the maximum level of flow reach its critical limit.

Let $\{n_H\}$ be the set of malicious flow, the probability of choosing a normal flow i is given below:

$$\Pr(\overline{mali}) = n - n\,H \,/\, n$$

Hence the probability of choosing an innocent flow is given by

$$\Pr(m) = \Pr(\in i \cap (\overline{mali}))$$

Since the events are independent so

$$\Pr(m) = \text{pr}(\in i) * p\ (\overline{mali})$$

## Severity check module

The role of this module is to check the intensity level of flooding attacks by classifying into medium, high and severe. Once a flooding attack is detected, the RCFDAT checks the status of the resources. One of the indications of an ongoing flooding attack is a rapid increase in the utilisation of available resources such as bandwidth and computation. This module contains different profiles. The general format of the profiles is given in table 2.

Where Tru is the average value of utilisation, which can be calculated as

Tru = CPU Utilisation + Bandwidth consumption / 2

The severity check module also classifies the particular attack and its consequences on the overall system performance regarding bandwidth and computation. The classification is given in table 3.

- The computed values {UF, M}, {UF, H}, and {UF, S} indicate that the UDP flooding attack is medium, high and severe in intensity respectively.
- {SF, M}, {SF, H}, and {SF, S} indicate that the SYN flooding attack is medium, high and severe in nature respectively.
- {IF, M}, {IF, H}, and {IF, S} express the same statistics for an ICMP flooding attack.
- The same type of classification is true for probe-request and de-authentication kinds of flooding attacks.

However, sometimes rapid resource utilisation may be due to software bugs, viruses, and worms like MS-blast. The severity check module classifies such cases as non-flooding anomalies, in which the traffic flows are normal, yet there is rapid increase in the utilisation of resources.

The severity check module works by using simple rules of IF-ELSE. The generic form of rules is such as:

| Profile | CPU | Bandwidth | Tru |
|---|---|---|---|
| Medium | 31–50 | 26–40 | 28.5–45 |
| High | 51–75 | 41–65 | 46–70 |
| Severe | Above 76 | Above 66 | Above 71 |

Table 2: Severity check using profiles.

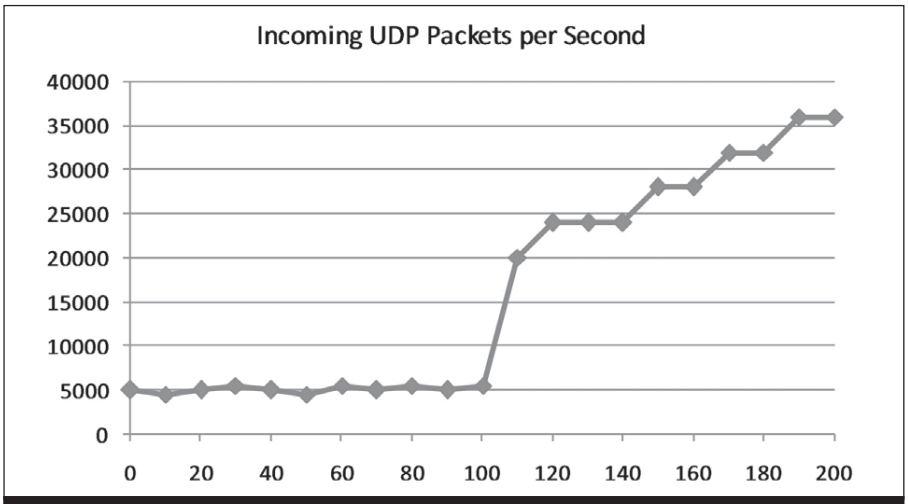


Figure 3: Incoming UPD packets/second.

- IF ALL values (CPU, bandwidth, Tru) are below MEDIUM profile, THEN resource utilisation is NORMAL and the condition is good.
- IF ALL or MOST of these values have MEDIUM OR HIGH values THEN resource utilisation is MEDIUM or HIGH and it is problem.
- IF ANY of these values is in the SEVERE range THEN resource utilization is SEVERE and it is a disaster.

### Alarm module

The alarm module receives input from the severity check module, and raises separate types of alarms for flooding and non-flooding attacks to inform the appropriate controller.

## 5. Simulation results and discussion

To test the accuracy of our system, several simulations have been conducted. The bandwidth of all links is 10Mbps. Normal nodes generate traffic at the rate of 0.3 Mbps. For conducting a flooding attack Trible Flood Network 2000 (TFN2K) is used, which is a clients/daemons program that coordinates to launch a flooding attack (UDP, ICMP, SYN) against a victim machine. We analysed the traffic flows under different variations of flooding attacks. The use of resources was observed for severity. Total simulation duration was set to 200 seconds. In the first 100 seconds, normal traffic flow and resource utilisations were observed.

### UDP flood

The UDP flood was started from 100–200 seconds. As soon as the flood was started, some great variations were observed in traffic flow (packets/sec). The packets rate sharply increased once the flooding attack started, as shown in figure 3.

Under normal conditions (0–100 seconds), UDP traffic is below 5 000 packets/second. When a flooding attack is launched (100–200 seconds), the traffic flow sharply increases to 20000 packets/second. At the peak of an UDP flooding attack, the traffic flow is more than 35 000 packets/second. The RCFDAT immediately detects the flooding attack and contacts the severity module to check the severity. The severity module checks the use of resources. During normal conditions, both bandwidth and computations are below 30%. However, at the peak of a UDP flooding attack the Tru value reaches 60, which indicates high severity.

| | Medium profile (M) | High profile (H) | Severe profile (S) |
|---|---|---|---|
| UDP flood (UF) | UF, M | UF, H | UF, S |
| SYN flood (SF) | SF, M | SF, H | SF, S |
| ICMP flood (IF) | IF, M | IF, H | IF, S |
| Probe request flood (PF) | PF, M | PF, H | PF, S |
| De-authentication flood (DF) | DF, M | DF, H | DF, S |

Table 3: Classification analysis.

### SYN flood

In a normal environment, the TCP SYN and FIN rates are almost consistent. However, when a SYN flood is started from 100–200 seconds great variations are observed both in FIN and SYN rates as shown in figure 4.

Under normal conditions (0–100 seconds), the SYN and FIN ratios are approximately consistent. However, during a SYN flooding attack, the variation is quite huge and it is this variation that indicates a SYN flooding attack. Once RCFDAT detects a SYN flooding attack it consults the severity check module. The utilisation of resources can be seen in figure 5.

We can see that the bandwidth utilisation of SYN and UDP in the flooding attack is approximately the same, however, the SYN flooding attack consumes more computational resources. Here the Tru is approximately 65, which again indicates high severity.

### Probe request and de-authentication flood

During a probe-request flooding attack, the probe-request flow suddenly increases. In normal circumstances, probe frames are in between 2–6 frames per second, however, during a flooding attack arriving probe frames show a sharp increase to 20–30 frames per second. However, in a de-authentication attack arriving frames do not increase sharply per second, as this kind of attack is launched to de-authenticate the legitimate users. If there are seven legitimate users currently using network resources, then in a de-authentication attack the adversary would send only seven de-authentication frames. This is the reason we do not observe a sharp increase in arriving frames. The RCFDAT analyses variations in the arriving frames, sequence number, MAC address, and the time interval to detect this kind of attack.

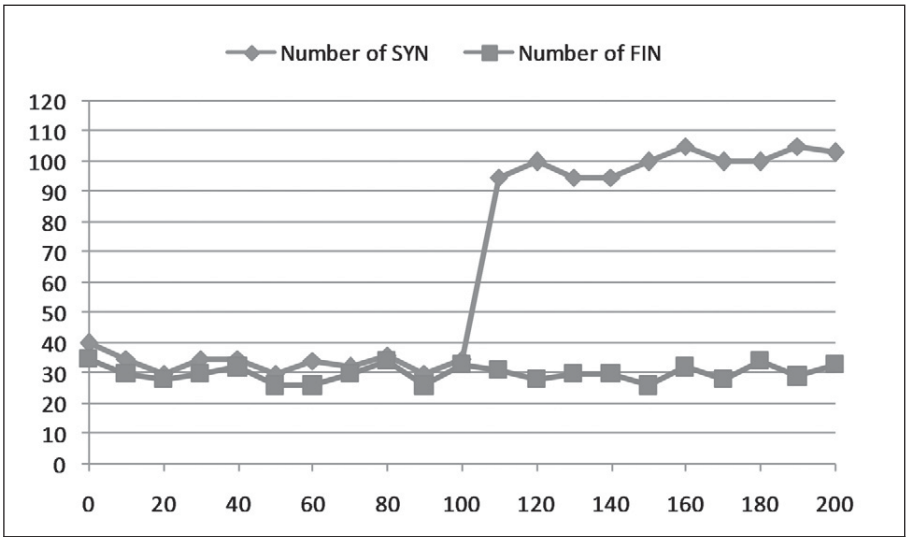


Figure 4: TCP flag rates.

| Attack type | Detection rates | False alarm rates |
|---|---|---|
| Non flooding | 99.72% | 0.4% |
| UDP flood | 97.54% | 1.7% |
| SYN flood | 99.5% | 0.2% |
| ICMP flood | 95.62% | 2.9% |
| IGMP flood | 95.75% | 3.1% |
| Probe request flood | 89.67 | 7.48 |
| De-authentication | 86.38 | 8.79 |

Table 4. Flooding attacks detection rate of RCFDAT.

De-authentication attacks are not so costly in terms of computation and bandwidth utilisation. However, probe-request flooding attacks are medium in computational severity.

The overall detection rates of RCFDAT are given in table 4. The results show that RCFDAT has the capability to detect a variety of flooding attacks with maximum accuracy having low false alarms.

Keeping in mind the statistics given in table 4, it is clear that the RCFDAT has a satisfactory detection rate in terms of different multi-layered flooding attacks.

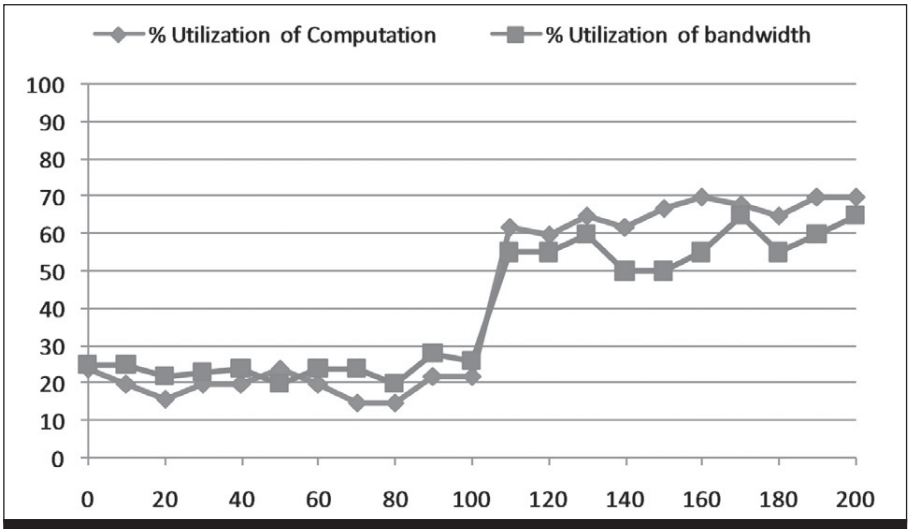


Figure 5: Utilisation of resources during SYN flooding attack.

## 6. Conclusions

In this paper, a cross-layered approach for detecting multi-layered flooding attacks is proposed. The theoretical fundamentals have been checked with the help of simulations to test the accuracy of the proposed RCFDAT mechanism. To maximise the detection rate and minimise the false alarms ratio, RCFDAT observed traffic flow variations because the first sign of any flooding attack is a sharp increase in traffic flow. Once the flooding attack has been detected, the candidate mechanism observes the utilisation of the resources such as computational overheads and bandwidth consumption to check the severity and intensity of the flooding attack, measured as medium, high or severe. Conversely, if the traffic flow is normal and great variations are observed nonetheless in resource utilisations, then such an anomaly is classified as non-flooding. RCFDAT raises different sort of alarms to demonstrate the attack type.

## References

1. S. Northcutt, J. Novak: Network intrusion detection. SAMS. 3rd edn., ISBN: 0735712654, 2002.
2. M. Hamdi, N. Boudriga: Detecting denial of service attacks using the wavelet transform, Elsevier Computer Communications, Vol. 30, pp. 3203–3213, 2007.
3. D. Moore, G.M. Voelker, S. Savage: Inferring internet Denial of Service activity. Proc. of the 10th USENIX Symposium, pp. 9–22, 2001.
4. P. Mutaf: Defending against a Denial of Service attack on TCP. Proc. of the 2nd International Workshop on Recent Advances in Intrusion Detection, 1999.
5. M. Lyu, L. Lau: Firewall security: Policies, testing and performance evaluation. Proc. of the 24th International Conference on Computer Software and Applications (COMPSAC), pp. 116–121, 2000.
6. P. Ferguson, D. Senie: Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, 2000.
7. Sans institute: Egress filtering. Nov. 2008 <www.sans.org/y2k/egress.htm>
8. Y. Xiong, S. Liu, P. Sun: On the defense of the distributed denial of service attacks:

An on-off feedback control approach, IEEE Transactions on Systems, Man, and Cybernetics Part A, Systems and Humans, Vol. 31, No. 4, pp. 228–293, July 2001.
9. G. Badishi, I. Keidar, A. Sasson: Exposing and eliminating vulnerabilities to denial of service attacks in secure gossip-based multicast, IEEE Transactions on Dependable and Secure Computing. Vol. 3, No. 1, pp. 45–61, January–March 2006.
10. T.M. Gil, M. Poletto: Multops. A data structure for bandwidth attack detection. Proc. of the 10th USENIX Symposium, pp. 23–38, 2001.
11. A. Householder, A. Manion, L. Pesante, G.M. Weaver: Meaning the threat of denial of service attacks. CERT Coordination Centre, White Paper, 2001.
12. A.B. Kulkarni, S.F. Bush, S.C. Evans: Detecting Denial of Service attacks using Kolmogorow complexity metrics. Technical report CRD176, GE Research and Development Centre, 2001.
13. K. Park, H. Lee: On the effectiveness of route based packet filtering for distributed DoS attack prevention in power-law internets. Proc. of ACM (SIGCOMM), 2001.
14. Kent, W.T. Strayer: Hash-based IP traceback. Proc. of ACM (SIGCOMM), 2001.
15. D.X. Song, A. Perring: Advanced and authenticated marking schemes for IP traceback. Proc. of the IEEE Information and Communications (Infocom), 2001.
16. S. Malliga, A. Tamilarasi: A defensive mechanism to defend against DoS/DDoS attacks by IP traceback with DPM. Proc. of the International Conference on Computational Intelligence and Multimedia Applications, 2007.
17. T. Peng, C. Leckie, K. Ramamohanarao: Protection from distributed denial of service attacks using history-based IP Filtering, Proc. of the IEEE, 2003.
18. A. Ramanathan: WADeS. A tool for distributed denial of service attack detection. TAMU-ECE, Master of Science thesis, 2002.
19. H. Wang, D. Zhang, K.G. Shin: Detecting SYN flooding attacks. Proc. of IEEE INFOCOM, pp. 1530–1539, 2002.
20. S. Noh, G. Jung, K. Choi, C. Lee: Compiling network traffic into rules using soft computing methods for the detection of flooding attacks. Elsevier, Applied Soft Computing, Vol. 8, pp. 1200–1210, 2008.
21. A. Kuzmanovic, E.W. Knightly: Low rate TCP targeted denial of service attacks and counter strategies. IEEE/ACM Transactions on Networking, Vol. 14, No. 4, pp. 683–696, August 2006.
22. S. Seufert, D. O'Brien: Machine learning for automatic defence against distributed denial of service attacks. IEEE International Conference on Communications, 2007.
23. F. Ferreri, M. Bernaschi, L. Valcamonici: Access point vulnerabilities to DoS attacks in 802.11 networks. IEEE Wireless Communications and Networking Conference, March 2004.
24. Y. Bouzida, F. Cuppens, S. Gombault: Detecting and reacting against distributed denial of service attacks. IEEE International Conference on Communications (ICC), pp. 2394–2400, 2006.
25. F. Lau, S.H. Rubin, M.H. Smith, L. Trajkovic: Distributed Denial of Service attacks. IEEE International Conference on Systems, Man and Cybernetics, pp. 2275–2280, 2000.
26. J. Bellardo, S. Savage: 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions. Proc. of the 12th USENIX security symposium, pp.15–28, August 2003.
27. J. Felix, C. Joseph, A. Das, B.-C. Seet, B.-S. Lee: Cross-layer versus single layer approaches for intrusion detection in MANETs. Proc. of the IEEE, ICON 2007.
28. M. Malekzadeh, A.Z.A. Ghani, Z.A. Zulkarnain, Z. Muda: Security improvement for management frames in IEEE 802.11 wireless networks, International Journal of Computer Science and Network Security, Vol. 7, No. 6, June 2007.
29. J. Wright: Detecting wireless LAN MAC address spoofing. White Paper, 2003. May 2009 <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>

# Joining the dots

**Richard Walters, product director, Overtis Systems**

**Data loss continues to grab the headlines. For those of us in the information security industry, these stories are testament to the fact that we are failing. Data is being removed intentionally, and disseminated unintentionally, from UK organisations on an unprecedented scale. Examples we've seen range from gaining physical access to restricted areas (through access card theft, lack of anti-passback on turnstiles, and plain simple tailgating), to data theft over instant messenger using file transfer, and social networking sites (uploading a file from the corporate network during office hours, and downloading it to another location later).**


Richard Walters

In one case, an office multi-function device (MFD) was used to scan sensitive documents to PDF and email them direct to an external recipient by entering their email address on the LCD screen of what was essentially a sophisticated photocopier. In another, a customer services manager asked all team members for their passwords just in case anything arose when they were off sick or on holiday, subsequently using those accounts to defraud the company of hundreds of thousands of pounds.

## Data leakage vectors

The number of data leakage vectors available to the internal user is increasing. Removable media and email are reasonably well addressed, while other vectors